



## TACACS+ Commands

This chapter describes the commands used to configure TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.



**Note**

Refer to the chapter “Authentication Commands”, the chapter “Authorization Commands”, and the chapter “Accounting Commands” for information about commands specific to AAA.

For information on how to configure TACACS+, refer to the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the section “TACACS+ Configuration Examples” located at the end of the chapter “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.



**Note**

TACACS and Extended TACACS commands are included in Cisco IOS Release 12.2 software for backward compatibility with earlier Cisco IOS releases; however, these commands are no longer supported and are not documented for this release.

Cisco recommends using only the TACACS+ security protocol with Release 12.1 and later of Cisco IOS software. For a description of TACACS and Extended TACACS commands, refer to the chapter “TACACS, Extended TACACS, and TACACS+ Commands” in Cisco IOS Release 12.0 *Security Command Reference* at Cisco.com.

[Table 16](#) identifies Cisco IOS software commands available to the different versions of TACACS. Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, Extended TACACS, and TACACS+. TACACS and Extended TACACS commands that are not common to TACACS+ are not documented in this release.

**Table 16 TACACS Command Comparison**

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
<b>aaa accounting</b> <sup>1</sup>	–	–	yes
<b>aaa authentication arap</b> <sup>1</sup>	–	–	yes
<b>aaa authentication enable default</b> <sup>1</sup>	–	–	yes
<b>aaa authentication login</b> <sup>1</sup>	–	–	yes
<b>aaa authentication ppp</b> <sup>1</sup>	–	–	yes

Table 16 TACACS Command Comparison (continued)

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa authorization <sup>1</sup>	–	–	yes
aaa group server tacacs+			yes
aaa new-model <sup>1</sup>	–	–	yes
arap authentication <sup>1</sup>	–	–	yes
arap use-tacacs	yes	yes	–
enable last-resort	yes	yes	–
enable use-tacacs	yes	yes	–
ip tacacs source-interface	yes	yes	yes
login authentication <sup>1</sup>	–	–	yes
login tacacs	yes	yes	–
ppp authentication <sup>1</sup>	yes	yes	yes
ppp use-tacacs <sup>1</sup>	yes	yes	–
server	–	–	yes
show tacacs	—	—	yes
tacacs-server attempts	yes	–	yes
tacacs-server authenticate	yes	yes	–
tacacs-server directed-request	yes	yes	yes
tacacs-server extended	–	yes	–
tacacs-server host	yes	yes	yes
tacacs-server key	–	–	yes
tacacs-server last-resort	yes	yes	–
tacacs-server notify	yes	yes	–
tacacs-server optional-passwords	yes	yes	–
tacacs-server retransmit	yes	yes	–
tacacs-server timeout	yes	yes	–

1. These commands are documented in separate chapters. Refer to the appropriate authentication, authorization, or accounting section of the *Cisco IOS Security Command Reference*, or use the index to locate a command.

# aaa group server tacacs+

To group different server hosts into distinct lists and distinct methods, use the **aaa group server tacacs+** command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

```
aaa group server tacacs+ group-name
```

```
no aaa group server tacacs+ group-name
```

## Syntax Description

<b>tacacs+</b>	Uses only the TACACS+ server hosts.
<i>group-name</i>	Character string used to name the group of servers.

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(5)T	This command was introduced.

## Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

## Examples

The following example shows the configuration of an AAA group server named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
  server 1.1.1.1
  server 2.2.2.2
  server 3.3.3.3
```

## Related Commands

Command	Description
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security.
<b>aaa authentication login</b>	Enables AAA accounting of requested services for billing or security purposes.
<b>aaa authorization</b>	Sets parameters that restrict user access to a network.

<b>Command</b>	<b>Description</b>
<b>aaa new-model</b>	Enables the AAA access control model.
<b>tacacs-server host</b>	Specifies a TACACS+ host.

# ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

**ip tacacs source-interface** *subinterface-name*

**no ip tacacs source-interface**

## Syntax Description

<i>subinterface-name</i>	Name of the interface that TACACS+ uses for all of its outgoing packets.
--------------------------	--

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.

## Usage Guidelines

Use this command to set a subinterface's IP address for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS+ reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the *up* state.

## Examples

The following example makes TACACS+ use the IP address of subinterface s2 for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

Related Commands	Command	Description
	<b>ip radius source-interface</b>	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
	<b>ip telnet source-interface</b>	Allows a user to select an address of an interface as the source address for Telnet connections.
	<b>ip tftp source-interface</b>	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

## server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

**server** *ip-address*

**no server** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the selected server.
---------------------------	-------------------	------------------------------------

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	TACACS+ group server configuration
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)T	This command was introduced.

<b>Usage Guidelines</b>	<p>You must configure the <b>aaa group server tacacs</b> command before configuring this command.</p> <p>Enter the <b>server</b> command to specify the IP address of the TACACS+ server. Also configure a matching <b>tacacs-server host</b> entry in the global list. If there is no response from the first host entry, the next host entry is tried.</p>
-------------------------	--

<b>Examples</b>	The following example shows server host entries configured for the RADIUS server:
-----------------	---

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
    server 1.0.0.1
    server 2.0.0.1
tacacs-server host 1.0.0.1
tacacs-server host 2.0.0.1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa new-model</b>	Enables the AAA access control model.
	<b>aaa server group</b>	Groups different server hosts into distinct lists and distinct methods.
	<b>tacacs-server host</b>	Specifies a RADIUS server host.

# show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in EXEC configuration mode.

**show tacacs**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.

**Examples** The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server      : 172.19.192.80/49
    Socket opens:      3
    Socket closes:     3
    Socket aborts:     0
    Socket errors:     0
    Socket Timeouts:   0
    Failed Connect Attempts: 0
    Total Packets Sent: 7
    Total Packets Recv: 7
    Expected Replies:  0
    No current connection
```

[Table 17](#) describes the significant fields shown in the display.

**Table 17** *show tacacs Field Descriptions*

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; that is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.

**Table 17** *show tacacs Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Expected replies	Number of outstanding replies from the TACACS+ server.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>tacacs-server host</b>	Specifies a TACACS+ host.

# tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

**tacacs-server directed-request** [**restricted**] [**no-truncate**]

**no tacacs-server directed-request**

## Syntax Description

<b>restricted</b>	(Optional) Restrict queries to directed request servers only.
<b>no-truncate</b>	(Optional) Do not truncate the @hostname from the username.

## Defaults

Disabled

## Command Modes

Global configuration

## Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

This command sends only the portion of the username before the “@” symbol to the host specified after the “@” symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the “@” symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the “@” symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

---

**Examples**

The following example disables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

## tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

```
tacacs-server host {host-name | host-ip-address} [key string] [nat] [port [integer]]
[single-connection] [timeout [integer]]
```

```
no tacacs-server host {host-name | host-ip-address}
```

### Syntax Description

<i>host-name</i>	Name of the host.
<i>host-ip-address</i>	IP address of the host.
<b>key</b>	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command <b>tacacs-server key</b> for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.
<b>nat</b>	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
<b>port</b>	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
<b>single-connection</b>	(Optional) Maintains a single open connection between the router and the TACACS+ server.
<b>timeout</b>	(Optional) Specifies a timeout value. This overrides the global timeout value set with the <b>tacacs-server timeout</b> command for this server only.
<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

### Defaults

No TACACS+ host is specified.

### Command Modes

Global configuration

### Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The <b>nat</b> keyword was added.
12.2(8)T	The <b>nat</b> keyword was integrated into Cisco IOS Release 12.2(8)T.

### Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key**, **single-connection**, and **nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

### Examples

The following example specifies a TACACS+ host named Sea\_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea\_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a\_secret.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

### Related Commands

Command	Description
<b>aaa authentication</b>	Specifies or enables AAA authentication.
<b>aaa authorization</b>	Sets parameters that restrict user access to a network.
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security.
<b>ppp</b>	Starts an asynchronous connection using PPP.
<b>slip</b>	Starts a serial connection to a remote host using SLIP.
<b>tacacs-server key</b>	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

# tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

**tacacs-server key** *key*

**no tacacs-server key** [*key*]

<b>Syntax Description</b>	<i>key</i>	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.
---------------------------	------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1	This command was introduced.

<b>Usage Guidelines</b>	<p>After enabling authentication, authorization, and accounting (AAA) with the <b>aaa new-model</b> command, you must set the authentication and encryption key using the <b>tacacs-server key</b> command.</p> <p>The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.</p>
-------------------------	--

<b>Examples</b>	<p>The following example sets the authentication and encryption key to “dare to go”:</p> <pre>tacacs-server key dare to go</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa new-model</b>	Enables the AAA access control model.
	<b>tacacs-server host</b>	Specifies a TACACS+ host.